PATENT APPLICATION

of

ROBERT WILMER RODENBECK

ROGER KEITH RUSSELL

and

MICHAEL LEE LONG

for

WIRELESS SECURITY CONTROL SYSTEM

Client Reference B-263

Attorney Docket 3054-74724

WIRELESS SECURITY CONTROL SYSTEM

[0001] This application is a continuation of U.S. Patent Application Serial No. 09/523,670, filed March 10, 2000, which claims the benefit of Provisional Application Serial No. 60/124,324, filed March 12, 1999, which applications are hereby incorporated by reference herein.

BACKGROUND AND SUMMARY OF THE INVENTION

[0002] The present invention relates to a security control system. More particularly, the present invention relates to a wireless security control system that grants or denies access to a user seeking access through a door.

[0003] In the access control and security industries, there are two types of access control systems: on-line systems and standalone systems. On-line systems perform access grant and deny functions and history recording and provide continuous monitoring of a secured door or portal with nearly instantaneous updating of user access privileges. Standalone systems perform many of the basic functions of on-line systems (access grant & deny, history recording, etc.) but generally do not provide continuous monitoring or instantaneous updating of user access privileges.

[0004] On-line systems cost three to four times more than standalone systems mainly because hard-wired connections are required to connect readers, sensors, and locking devices at the door to either a "panel" or central computer. The use of wires allows for continuous monitoring and instantaneous updating of user data, but at an inflated cost. Standalone systems maintain a cost advantage by being battery-powered and avoiding the use of wires. The main disadvantage of traditional Standalone systems is that if the user data needs to be updated, an individual must walk to and physically connect to the Standalone systems. Once connected, new user data can be downloaded into the system via a laptop, palmtop, or custom programming device.

[0005] Through the use of wireless radio frequency ("RF") technology, the present standalone security systems can perform user data updates and some monitoring on an as required basis. For RF wireless technology to be effectively implemented on standalone systems, battery power must be conserved. In preferred embodiments, the standalone system should maintain an appealing physical appearance. For example, any antennas should be hidden or unobtrusive.

[0006] A remote access control system includes a remote wireless communicator to receive wireless information from a central access control system. It also includes a remote access controller electrically coupled to the remote wireless communicator. The remote access controller would receive information from the remote wireless communicator and uses the information to control locking and unlocking of the door. The remote wireless communicator includes an antenna. A receiver housing is providing having an inner portion mounted to the inside of the door and an outer portion mounted outside of the door. The antenna is mounted to the outer portion of the housing and the remote wireless communicator and remote access controller are mounted to the inner portion of the housing. The remote wireless communicator also transmits wireless information to the central access control system and a switch is provided for selectively choosing between the receiving and transmitting the wireless information. A local communication port is coupled to the remote access controller to provide wired communication from a portable device. The remote wireless communicator communicates via RF information and preferably spread-spectrum RF.

[0007] The remote access control system also includes a reader to read user data when presented to the reader. The remote access controller determines whether the data is valid to control the locking and unlocking of the door. A battery is coupled to the reader, the remote access controller and the remote wireless communicator. The remote access communicator selectively connects the battery to the remote wireless communicator to conserve energy. The reader is mounted to the outer portion of the housing. The user data is provided on a token control card presented to the reader.

[0008] The central access security system includes the remote access system and a central access control system. The central access control system has a central access controller and a central wireless communicator. The central wireless communicator communicates with the remote wireless communicator. The central access controller is coupled to the central access communicator by a bus. The bus may be a wired network using network protocol, fiber optics, or a wireless bus. The system may include a plurality of central wireless communicators coupled to the bus and the central access controller. Each central wireless communicator may communicate wirelessly with one or more remote wireless communicators.

[0009] Other objects, advantages and novel features of the present invention will become apparent from the following detailed description of the invention when considered in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Fig. 1 is a diagrammatical view of a wireless security control system showing the wireless security control system including a central access control system and a plurality of remote access control systems or locksets mounted to a plurality of doors located remotely from the central access control system, the remote access control systems being configured to control the locking and unlocking of the respective door to allow only users having a valid token to pass through the door, and showing the central access control system communicating wirelessly with one or more of the remote access control systems to program the respective remote access control system and/or to receive user access information from the respective remote access control system;

[0011] Fig. 2 is a block diagram of the wireless security control system of Fig. 1 showing the central access control system of Fig. 1 having a central access controller and a central wireless communicator and each remote access control system of Fig. 1 having a remote wireless communicator, a remote access controller, a lock mechanism, and a token reader, the token reader being configured to read token data from the token, the remote access controller being configured to lock and unlock the lock mechanism, and the central and remote wireless communicators being configured to communicate information wirelessly between the central access controller and the remote access controller;

[0012] Fig. 3 is a perspective view of the wireless security control system of Figs. 1 and 2 showing an exploded perspective view of the remote access control system, the remote access control system being configured to communicate wirelessly with the central access control system and through a hard-wired connection with a portable access control system via a local communication port mounted to the remote access controller, and the remote access control system including a housing having a pair of plates positioned on opposite sides of the door to mount the remote access control system to the door;

[0013] Fig. 4 is a block diagram of the wireless security control system of Fig. 3, showing the remote access control system including the token reader, the remote access controller, the remote wireless communicator, the lock mechanism, a power source, and a user history module, the remote wireless communicator having a transmit/receive circuit and an antenna, the transmit/receive circuit having a transmitter, a receiver, and a switch to allow the remote access controller to communicate wirelessly with the central wireless communicator, and the remote access controller being configured to control the locking and unlocking of the lock mechanism and to communicate with the portable access control system.

DETAILED DESCRIPTION OF THE DRAWINGS

[0014] A wireless security control system 10 is shown in Fig. 1. The wireless security control system 10 controls whether a particular user 12 will be granted or denied access through a particular door 14. As shown in Fig. 1, user 12 is granted access by the wireless security control system 10 to pass through one of the doors 14 because user 12 properly presented a valid user data on a token 13 for example, to a remote access control system 22 mounted on door 14 which allowed user 12 to open door 14.

[0015] The wireless security control system 10 of the present invention includes a central access control system 20 and a plurality of remote access control systems 22 located remotely from central access control system 20. The central access control system 20 uses wireless communication technology to communicate with each remote access control system 22. The central access control system 20 can therefore be used to program each remote access control system 22 so that certain users are granted access through certain doors 14 and other users 12 are granted access through other doors 14. The central access control system 20 can also receive information from each remote access control system 22 so that user access information such as the time and date that a particular user 12 was granted access through door 14 can be tracked and monitored.

[0016] Each remote access control system or electronic lockset 22 is mounted to a respective door 14 to control whether the particular user 12 is granted or denied access through the particular door 14, as shown in Fig. 1. Remote access control system 22 will grant user 12 access through door 14 if user 12 properly presents valid user data for example on a token 13 to remote access control system 22. If the data on token 13 is deemed by remote access control system 22 to be valid, a lock mechanism 15 mounted to door 14 will be unlocked and the user will be granted access to pass through door 14, as shown in Fig. 1. However, if remote access control system 22 deems user data on token 13 to be invalid, or if token 13 is not properly presented to remote access control system 22, lock mechanism 15 on door 14 will remain locked and user 12 will not be granted access through door 14.

[0017] As shown illustratively in Fig. 1 and diagrammatically in Fig. 2, central access control system 20 includes a central access controller 30, a central wireless communicator 32, and a power and/or signal bus 36 that electrically interconnects central access controller 30 and central wireless communicator 32. Central wireless communicator 32 allows information to be communicated wirelessly between central access controller 30 and each remote access controller 22. The central access controller 30 is configured to communicate bidirectionally with one or more central wireless communicators 32, as shown in Fig. 2 by a double-headed arrow 34 interconnecting central access controller 30 and central wireless communicator 32. This bidirectional communication allows information to be transmitted from central access controller 30 to central wireless communicator 32 and/or received by central access controller 30 from central wireless communicator 32.

[0018] As shown in Fig. 1, bus 36 can simply be a hard wire connection between central access controller 30 and central wireless communicator 32. However, as shown diagrammatically in Fig. 4, bus 36 can also electrically interconnect central access controller 30 and central wireless communicator 32 using RF technology, fiber optics, coaxial cable, A/C power line, regular wire, twisted pair wire, or any other suitable electrical connection. A variety of different protocols such as CE bus, LON works<, TCP/IP, IPX/SPX, or custom protocols, can be used to transfer information from central access controller 30 to a plurality central wireless communicators 32 over one of the electrical connections mentioned above. Each

central wireless communicator 32 communicates wirelessly with one or more remote access control system 22.

[0019] Each remote access control system 22 is configured to communicate wirelessly and bidirectionally with one of the central wireless communicators 32 of central access control system 20, as shown in Fig. 2 by a double-headed arrow 58 interconnecting central wireless communicator 32 and remote access control system 22. As shown in Fig. 2, each remote access control system 22 includes a remote wireless communicator 60, a remote access controller 62, a user input device or token reader 64, and lock mechanism 15. The remote wireless communicator 60 is configured to communicate information wirelessly and bidirectionally to/from central wireless communicator 32. Because central and remote wireless communicators 32, 60 communicate wirelessly with one another, each remote access control system 22 can be a standalone unit which is located remotely from central access control system 20, as shown illustratively in Fig. 1. In other words, each remote access control system 22 does not have to be connected to central access control system 20 using hard-wire connections. Therefore, wire for connecting a remote access control system mounted to a door with a central access control system does not have to be pulled in a building where the wireless security control system 10 is installed.

[0020] Remote access controller 62 is configured to communicate bidirectionally with remote wireless communicator 60, as shown in Fig. 2 by double-headed arrow 68. Thus, remote access controller 62 can send or receive information to or from central access controller 30 through remote and central wireless communicators 60, 32. This allows remote access controller 62 to send periodic user access information to central access controller 30 while also allowing central access controller 30 to change the programming of remote access controller 62 by, for example, determining which tokens 13 have access to which doors 14.

[0021] As shown in Fig. 2, token reader or user input device 64 is adapted to read data stored on token 13 and transmit the data to remote access controller 62. If the data from token 13 is determined by the remote access controller 62 to be valid, the remote access controller 62 will send an "unlock" signal to lock mechanism 15 mounted to door 14. With lock mechanism 15 in an unlocked position, user 12 is able to open door 14. Token reader 64 can be a card reader as shown in Fig. 1, or any other device which interprets token data to permit an authorized user to access a

controlled door. For example, token reader 64 may be a keypad configured to receive token or user data by having user 12 key in a particular code, or a fingerprint reader configured to read a user's fingerprint which serves as the user data, or a retinal scanner configured to read a user's retina which serves as the user data. In addition, token reader 64 may be, for example, any of the following types of readers: magnetic stripe, proximity card, smart card, touch memory, and biometric which includes handprint, eye, facial recognition, facial blood flow, and voice.

[0022] As mentioned above, information can be communicated wirelessly from central access control system 20 to remote access control system 22 to allow central access control system 20 to program remote access control system 22. Basically, this involves central access controller 30 sending information to remote access controller 62 via central and remote wireless communicators 32, 60. This type of wireless communication allows the remote access control system 22 to be programmed by the central access control system 20 so that remote access controller 62 locks and unlocks door 14 only for approved users 12 having approved tokens 13 as directed by central access controller 30.

[0023] Information can also be communicated wirelessly from remote access controller 62 to central access control system 20. This involves a signal being sent from remote access controller 62 to central access controller 30 via remote and central wireless communicators 60, 32. This type of wireless communication allows user access information to be monitored and tracked by passing information received by remote access controller 62 from token reader 64 to central access controller 30.

[0024] A preferred embodiment of the wireless security control system 10 is shown in Fig. 3. As shown in Fig. 3, remote access control system 22 of wireless security control system 10 is mounted to door 14 to control the locking and unlocking of lock mechanism 15 which is also mounted to door 14. Remote access control system 22 includes a housing 69 having an outer plate or housing 73 and an inner plate or housing 74. Outer plate 73 mounts token reader 64 and antenna 71 to an exterior side of door 14. Antenna 71 may be mounted to either the interior or exterior side of door 14. Inner plate 74 mounts transmit/receive circuit 70, remote access controller 62, and a battery 66 to an interior side of door 14.

[0025] Outer and inner plates 73, 74 are each formed to include an aperture or hole 75, 76, respectively, to accommodate lock mechanism 15, as shown in Fig. 3.

Lock mechanism 15 is mounted to door 14 and is used to latch and lock door 14. Lock mechanism 15 includes an outer door handle 46, an inner door handle 47, a latch bolt retractor assembly 48, a latch bolt 49, and a spindle 50. Lock mechanism 15 is operable by means of either outer door handle 46 or inner door handle 47 to operate centrally-located latch bolt retractor assembly 48. The latch bolt retractor assembly 48 is mounted in door 14 and is connected to spring-biased latch bolt 49. Latch bolt retractor assembly 48 is electrically coupled to remote access controller 62 using a wire 91 so that control signals can be sent from remote access controller 62 to latch bolt retractor assembly 48 to move latch bolt retractor assembly 48 between a locked position and an unlocked position. In the unlocked position, latch bolt retractor assembly 48 can be operated by either inner or outer door handle 46, 47 to retract latch bolt 49 from its projected position (shown in Fig. 3) engaging a door frame (not shown) to a retracted position (not shown) lying inside door 14 and disengaging the door frame.

[0026] As shown in Fig. 3, spindle 50 is arranged to extend through latch bolt retractor assembly 48 and interconnect outer door handle 46 and inner door handle 47. When latch bolt retractor assembly 48 is in the unlocked position, rotation of either of the door handles 46, 47, rotates spindle 50 to operate latch bolt retractor assembly 48 and move latch bolt 49 from the projected position to the retracted position. Lock mechanism 15 is a mortise lockset. However, lock mechanism 15 could be any type of lock mechanism including, but not limited to: cylindrical lock mechanisms similar to those disclosed in U.S. Patent Nos. 5,590,555; 5,794,472; 5,421,178; and 4,428,212, which are incorporated herein by reference or mortise lock mechanisms similar to those disclosed in U.S. Patent Nos. 5,474,348; 4,589,691; and 4,389,061, which are incorporated herein by reference.

[0027] Inner plate 74 is also formed to include an opening 78 designed to allow access to various portions of remote access control system 22 during assembly or removal of remote access control system 22 to or from door 14, respectively. A cover (or cap) 77 is configured to cover opening 78 formed in inner plate 74 once remote access control system 22 is mounted to door 14.

[0028] As shown in Fig. 3, remote access controller 62 is mounted to inner plate 74 and is electrically coupled to token reader 64 by a wire 90. As discussed above, any suitable token reader may be used. As shown in Figs. 3 and 4, remote

wireless communicator 60 of remote access control system 22 includes a transmit/receive circuit 70, an antenna 71, and a wire 72 electrically interconnecting transmit/receive circuit 70 with antenna 71. As shown in Fig. 3, transmit/receive circuit 70 is mounted to inner plate 74 and antenna 71 is mounted to outer plate 73. Wire 72 extends through a hole 79 in door 14 to interconnect transmit/receive circuit 70 with antenna 71.

[0029] Transmit/receive circuit 70 is used to communicate (e.g., transmit and receive) information between remote access controller 62 and central wireless communicator 32 through antenna 71, as shown in Figs. 3 and 4. As shown in Fig. 4, transmit/receive circuit 70 includes a transmitter 80, a receiver 82, and a switch 84. Transmitter 80 is electrically coupled between remote access controller 62 and switch 84, as shown in Fig. 4, so that remote access controller 62 can transmit information through switch 84 and antenna 71 to central wireless communicator 32. Similarly, receiver 82 is electrically coupled between remote access controller 62 and switch 84 so that wireless information transmitted by central access controller 30 through central wireless communicator 32 can be received by remote access controller 62 through antenna 71 and receiver 82. Switch 84 simply disconnects the path between transmitter 80 and receiver 82 to prevent electrical overload of receiver 82.

[0030] Transmitter 80, receiver 82, and antenna 71 can be any variety of devices that cooperate to transmit and receive wireless information. For example, transmitter 80 and receiver 82 could use infrared, ultrasonic, magnetic, or radio frequency (RF). Preferably, as shown in Figs. 1 and 3, RF technology is used. For RF applications, antenna 71 could be a patch, loop, monopole, dipole whip, printed circuit whip (stub), helical (coil), chip, or slot antenna. As shown in Figs. 1 and 3, antenna 71 should maintain the aesthetic appeal of the unit while providing adequate RF performance. Switch 84 can also be a wide variety of switches for switching the flow of information from transmit to receive, or vice versa. For example switch 84 could be a specialized RF switch or PIN diodes.

[0031] There are many types of RF technology that could be used to configure transmitter 80 and receiver 82 for wireless communication. For example, the following types of RF technology could be used: frequency modulation (FM), amplitude modulation (AM), amplitude shift keying (ASK), frequency shift keying (FSK), phased shift keying (PSK), single band transmission, dual band transmission,

and spread spectrum transmission. Spread spectrum technology is resistant to interference, jamming, and multi-path fading. In the preferred embodiment, the 902-928 MHZ frequency range was selected because it is within the FCC spectrum. Spread spectrum technology makes communication between central wireless communicator 32 and remote wireless communicator 60 more reliable than the other RF transmission technologies mentioned above. In preferred embodiments, the present invention uses spread spectrum technology that is commercially available from Intellon Corp., located in Ocala, Florida. Familiar uses of spread spectrum technology include pagers, cordless telephones, and cellular telephones.

[0032] Battery 66 is mounted to inner plate 74, as shown in Fig. 3. Battery 66 provides power to remote access controller 62, token reader 64, and user history module 98, as shown in Figs. 3 and 4. Battery 66 also provides power to remote wireless communicator 60 through remote access controller 62. Remote access controller 62 includes a switch 67, as shown in Fig. 4, to control when power is applied to remote wireless communicator 60. Because battery 66 provides all the power required by remote access control system 22, the expense associated with pulling wires throughout a building to provide power to a remote access control system is eliminated. The remote access control system of the present invention could receive power by being hard-wired to a power source located away from door 14, but one of the cost advantages of remote access control system 22 would be lost by doing so. The major cost advantage is elimination of the wire connection between the remote access control system and the central access control system.

[0033] Remote access control system 22 is configured to conserve energy drawn from battery 66. This is done by checking for user updates periodically (once a day, once an hour, etc.) and reporting only high priority events to central access control system 20 on a real-time basis. This contrasts with continuously polling remote access control system 22 and communicating to central access control system 20 every time a decision is to be made.

[0034] The security control system 10 of the present invention allows for distributed decision making by having a single central access control system 20 and a plurality of remote access control systems 22. Distributed decision making is possible because each remote access control system 22 decides independently whether a particular user 12 or token 13 is granted or denied access through the door 14 to

which remote access control system 22 is coupled. The remote access control system 22 does not need authorization from central access control system 20 before making a decision. Therefore, the distributed decision making capability increases the speed of the decision making process because the remote access control system 22 makes the grant or deny decision locally, at the door 14, without having to communicate with central access control system 20.

[0035] The distributed decision making capability of security control system 10 also allows for better degrade mode performance. In other words, the distributed decision making capability prevents a failure of a single component from shutting down the entire security control system 10. For example, by having several remote access control systems 22 that make decisions independently from central access control system 20, the failure of a single component within a single remote access control system 22 or within the central access control system 20 is less likely to shut down the entire security control system 10 than if all the decision making were done by a central access control system.

[0036] The distributed decision making capability also minimizes power consumption of battery 66 in a wireless system since the remote access control system or lockset 22 does not have to power up the remote wireless communicator 60 every time a token 13 is presented to remote access control system 22. As mentioned above, remote wireless communicator 60 is powered up by remote access controller 62 only when wireless communication is desired and remains powered down during the normal access grant or deny decision making process. This contrasts with a centralized decision making system where wireless communication would be needed each time a token is presented to a remote lockset which would naturally reduce the life of the battery.

[0037] As shown in Figs. 3 and 4, remote access control system 22 may also include a local communication port 92 mounted to outer plate 73 and electrically coupled to remote access controller 62 by a wire 93 so that a transport device 94 can be connected to remote access control system 22. Transport device 94 is used to transfer information (such as configuration data) from the central access controller 30 to the remote access controller 62. For example, a security administrator would determine the user's access control privileges for a particular remote access control system or lockset 22. This information is normally kept at a central location, such as

the central access control system 20. When programming the remote access controller 62 is determined necessary, the administrator would transfer the information to transport device 94 (which could be a laptop, a palmtop, etc.), physically take the transfer device 94 to the remote access control system 22, connect the transport device 94 to the local communication port 92, and transfer data from the transport device 94 to remote access controller 62. Of course, the same data transfer could occur wirelessly through central and remote wireless communicators 32, 60.

[0038] Remote access control system 22 may also include a user history module 98, as shown in Fig. 4. User history module 98 allows remote access controller 62 to track information such as which tokens 13 were granted access through which doors 14 on what date and at what time. This user history information from module 98 can then be transmitted to either central access control system 20 or local access control system or transport device 94 on an as-needed basis or on a regularly-scheduled basis (such as once a day, once a week, or once a month).

[0039] In operation, user 12 presents user information on a token 13 to token reader 64. Presentation of token 13 to reader 64 is sensed by token reader 64 and activates or "wakes-up" remote access controller 62. An illustrative device for sensing a token reader with a wake-up circuit is disclosed in U.S. Patent Application Serial No. 09/243,772 entitled "Proximity Card Detection System," the disclosure of which is incorporated herein by reference. Token 13 is read by token reader 64 and user data (retrieved from the token) is sent to remote access controller 62. Remote access controller 62 evaluates the user data and performs an access grant or deny decision. If an access grant decision is made, remote access controller 62 applies an unlocking signal to lock mechanism 15 and allows user 12 to gain access through door 14. After a predetermined period of time, a locking signal is applied to lock mechanism 15 to re-lock door 14. If an access deny decision is made, no action is taken on lock mechanism 15. The results of the transaction are stored in user history 98 contained in remote access controller 62.

[0040] On a predetermined time period (minute, hour, day, week), remote access controller 62 is activated by a real-time clock. Activation of remote access controller 62 for this particular reason initiates a data transfer via RF from remote access control system 22 to central access control system 20. Remote access control

system 22 inquires for any updates to the user database and transfers any transaction history events requested by central access control system 20.

[0041] In the case of user updates, remote access control system 22 switches into the RF receive mode and processes data received from central access control system 20. This data is transferred into the user memory 98 of remote access control system 22 and stored. If central access control system 20 requested history transaction information, remote access control system 22 recalls information from the history or user memory 98 and transmits the data via RF to central access control system 20.

[0042] When data transmission from remote access control system 22 to central access control system 20 is desired, data from remote access controller 62 is processed and modulated using spread spectrum techniques and communicated through antenna 71. This data is received by central wireless communicator 32 and demodulated back into a digital data stream. This data stream is passed along to central access controller 30 and processed. Information is passed along via a series of commands and protocols similar to those used by LAN networks, as described above.

[0043] Conversely, when central access controller 30 wishes to communicate with remote access controller 62, a data stream is transmitted from central access controller 30 to central wireless communicator 32. The data is modulated using spread spectrum techniques and communicated through central wireless communicator 32. This data is received by remote wireless communicator 60 and demodulated back into a digital data stream. This data stream is passed along to remote access controller 62 and processed.

[0044] By combining RF wireless technology with a battery powered access control system, the elimination of wires in standard access control products is eliminated or greatly reduced. Additionally, because remote access controller 62 contains intelligence, remote access controller 62 can make all access control decisions at the door. This intelligence eliminates the need to transmit and/or receive data via RF for each event that occurs at the door. This feature greatly reduces the amount of power draw required by a battery powered device.

[0045] Although the invention has been described in detail with reference to certain preferred embodiments, variations and modifications exist within the scope and spirit of the invention as described and defined in the following claims.